UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/029,070	12/21/2001	Charles M. Patton	10013446-1	5339

7590 12/13/2005

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
DARROW, JUSTIN T	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 12/13/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	10/029,070	PATTON ET AL.
	Examiner	Art Unit
	Justin T. Darrow	2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-51* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-51* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 December 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-51 have been examined.

Information Disclosure Statement

2. The information disclosure statements (IDSes) submitted on 10/06/2003 and 03/12/2002 were filed before the mailing date of the first Office action on the merits The submissions are in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Specification

3. The disclosure is objected to because of the following informalities:

¶ [0001], lines 2-3, delete "_____ and _____ (docket numbers 10013492 and 10013447)," and replace with --10/029,338, filed 12/21/2001, and 10/028,808, filed 12/21/2001,--.

Appropriate correction is required.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1-51 are rejected under 35 U.S.C. 102(e) as being anticipated by Pearce et al., U.S. Patent No. 6,243,468 B1.

As per claim 1, Pearce et al. illustrates a method for securing ownership for a two-part device with a physical unit and a virtual unit, comprising:

initiating, by a user, an activation signal from the physical unit to the virtual unit to activate an ownership procedure (see column 5, lines 30-39; figure 2; the user enters a portion of the product ID (PID) that is combined with another portion in the software); and

utilizing a double safety mechanism to activate ownership services via the virtual unit for the physical unit (see column 5, lines 34-45; the product ID, unique to the specific installation, is registered with a registration authority).

As per claim 2, Pearce et al. also describes:

that the virtual unit is a virtual device hosting entity that is one of: an Internet Data Center, and e-Services Host, a Control Console, and a Secure Data Storage Unit (see column 4, lines 13-25; the software enables the computer to function as handheld computer, a Web-enabled television, an automation system within the privacy of the home).

As per claim 3, Pearce et al. further points out:

that the Control Console is a web enabled browser (see column 4, lines 13-15; the software enables the computer to function as a Web-enabled television).

As per claim 4, Pearce et al. then elaborates:

that the Secure Data Storage Unit is a memory controllable by the user (see column 4, lines 27-38; figure 3, item 42; the customer computer contains system memory).

As per claim 5, Pearce et al. then elaborates:

that the Secure Data Storage Unit is a physical device under control by the user (see column 4, lines 27-38; figure 3, item 42; the customer computer contains system memory).

As per claim 6, Pearce et al. also suggests:

that the Secure Data Storage Unit is a virtual device under control by the user (see column 4, lines 49-53; nonvolatile storage of computer readable instructions, data structures, program modules and other data).

As per claims 7-11, Pearce et al. additionally specifies:

that the double safety mechanism includes steps of:

upon the virtual unit upon being activated (see column 4, lines 46-48; for preparing the software product for installation and use on the computer), generating a first Knowledge Element and a first Proof of Knowledge Element (see column 5, lines 46-56; figure 4, step 150; a first Knowledge Element of information that identifies the software product, place of manufacture, and serial number and a first Proof of Knowledge Check Element manifested by a product ID consisting of a 5-bit registered product code value, a 3-bit site value indicating the place of manufacture, and a 7-bit serialized number incremented with each product);

storing the first Knowledge Element in a Secure Storage Unit (see column 5, lines 52-56; storing the registered product code for the software product, the site value indicating the place of manufacture, and the serial number for the product in a secure memory in the computer) and sending the Proof of Knowledge Check Element to the virtual unit (see column 6, lines 23-26; figure 4, step 154; receiving the 15-bit product ID to concatenate with the 5-bit hardware ID);

upon the virtual unit receiving the Proof of Knowledge Check Element (see column 6, lines 23-26; figure 4, step 154; receiving the 15-bit product ID to concatenate with the 5-bit hardware ID), storing, by the virtual unit the first Proof of Knowledge Check Element in an Ownership Proof of Knowledge Check Store (see column 6, lines 23-29; storing the 15-bit product ID in a memory for concatenation with the 5-bit hardware ID) and generating, by the virtual unit, a second Knowledge Element and a second Proof of Knowledge Check Element (see column 5, lines 57-67; column 6, lines 1-15; TABLE 1; figure 4, step 152; a second Knowledge Element of information that identifies a set of hardware components that make up the customer's computer and a second Proof of Knowledge Check Element represented by hardware ID (H/W ID) comprised of a bit sequence with the bit position indicative of the kind of component and a bit value indicative of an identifier of the component);

storing, by the virtual unit, the second Knowledge Element in an Ownership Knowledge Element Storage Unit (see column 6, lines 1-3; storing the bits used to form the 5-bit hardware ID in a memory);

sending, by the virtual unit, the second Proof of Knowledge Check Element to the physical unit (see column 6, lines 48-50; figure 4, step 160; sending the hardware ID processed into a registration ID to the customer computer); and

storing the second Proof of Knowledge Check Element in a second Proof of Knowledge Check Store unit (see column 6, lines 52-55; storing in system memory accessible by the software program).

As per claims 12 and 13, Pearce et al. then discusses:

utilizing an Internet address recorded in the physical unit to the activation signal (see column 6, lines 16-26; sending the product ID to a registration server over the Internet).

As per claim 14, Pearce et al. illustrates a method for taking ownership of a part-physical, part-virtual device, comprising the steps of:

communicating, by a physical unit of the device, by sending an activation signal to a virtual unit of the device (see column 5, lines 33-39; see figure 2, items 32 and 100; entering a portion of the product ID of the software product to activate the software to combine that portion with another portion already included in the software program);

registering ownership of the device (see column 6, lines 23-29; figure 4, step 154; a software product sending a 20-bit value over a network to a registration server to register itself with a registration authority; see column 5, lines 45-56; registering the software product for installation and use on the computer) using a double knowledge check-proof of knowledge check mechanism (see column 6, lines 23-26; figure 4, step 154; where the 20-bit value is derived from the concatenation of a 15-bit product ID and a 5-bit hardware ID, each representative of distinct information and proof of knowledge of that information: see column 5, lines 46-46; figure 4, step 150; a first Knowledge Element of information that identifies the

software product, place of manufacture, and serial number and a first Proof of Knowledge Check Element manifested by a product ID consisting of a 5-bit registered product code value, a 3-bit site value indicating the place of manufacture, and a 7-bit serialized number incremented with each product; see column 5, lines 57-67; column 6, lines 1-15; TABLE 1; figure 4, step 152; a second Knowledge Element of information that identifies a set of hardware components that make up the customer's computer and a second Proof of Knowledge Check Element represented by hardware ID (H/W ID) comprised of a bit sequence with the bit position indicative of the kind of component and a bit value indicative of an identifier of the component).

As per claim 15, Pearce et al. also describes:

that the virtual unit is a virtual device hosting entity that is one of: an Internet Data Center, and e-Services Host, a Control Console, and a Secure Data Storage Unit (see column 4, lines 13-25; the software enables the computer to function as handheld computer, a Web-enabled television, an automation system within the privacy of the home).

As per claim 16, Pearce et al. further points out:

that the Control Console is a web enabled browser (see column 4, lines 13-15; the software enables the computer to function as a Web-enabled television).

As per claim 17, Pearce et al. then elaborates:

that the Secure Data Storage Unit is a memory controllable by the user (see column 4, lines 27-38; figure 3, item 42; the customer computer contains system memory).

As per claim 18, Pearce et al. then elaborates:

that the Secure Data Storage Unit is a physical device under control by the user (see column 4, lines 27-38; figure 3, item 42; the customer computer contains system memory).

As per claim 19, Pearce et al. also suggests:

that the Secure Data Storage Unit is a virtual device under control by the user (see column 4, lines 49-53; nonvolatile storage of computer readable instructions, data structures, program modules and other data).

As per claims 20-24, Pearce et al. additionally specify:

that the double knowledge check-proof of knowledge check mechanism includes steps of:

upon the virtual unit upon being activated (see column 4, lines 46-48; for preparing the software product for installation and use on the computer), generating a first Knowledge Element and a first Proof of Knowledge Element (see column 5, lines 46-56; figure 4, step 150; a first Knowledge Element of information that identifies the software product, place of manufacture, and serial number and a first Proof of Knowledge Check Element manifested by a product ID consisting of a 5-bit registered product code value, a 3-bit site value indicating the place of manufacture, and a 7-bit serialized number incremented with each product);

storing the first Knowledge Element in a Secure Storage Unit (see column 5, lines 52-56;

storing the registered product code for the software product, the site value indicating the place of manufacture, and the serial number for the product in a secure memory in the computer) and sending the Proof of Knowledge Check Element to the virtual unit (see column 6, lines 23-26; figure 4, step 154; receiving the 15-bit product ID to concatenate with the 5-bit hardware ID);

upon the virtual unit receiving the Proof of Knowledge Check Element (see column 6, lines 23-26; figure 4, step 154; receiving the 15-bit product ID to concatenate with the 5-bit hardware ID), storing, by the virtual unit the first Proof of Knowledge Check Element in an Ownership Proof of Knowledge Check Store (see column 6, lines 23-29; storing the 15-bit product ID in a memory for concatenation with the 5-bit hardware ID) and generating, by the virtual unit, a second Knowledge Element and a second Proof of Knowledge Check Element (see column 5, lines 57-67; column 6, lines 1-15; TABLE 1; figure 4, step 152; a second Knowledge Element of information that identifies a set of hardware components that make up the customer's computer and a second Proof of Knowledge Check Element represented by hardware ID (H/W ID) comprised of a bit sequence with the bit position indicative of the kind of component and a bit value indicative of an identifier of the component);

storing, by the virtual unit, the second Knowledge Element in an Ownership Knowledge Element Storage Unit (see column 6, lines 1-3; storing the bits used to form the 5-bit hardware ID in a memory);

sending, by the virtual unit, the second Proof of Knowledge Check Element to the physical unit (see column 6, lines 48-50; figure 4, step 160; sending the hardware ID processed into a registration ID to the customer computer); and

storing the second Proof of Knowledge Check Element in a second Proof of Knowledge

Check Store unit (see column 6, lines 52-55; storing in system memory accessible by the software program).

As per claims 25 and 26, Pearce et al. then discusses:

utilizing an Internet address recorded in the physical unit to the activation signal (see column 6, lines 16-26; sending the product ID to a registration server over the Internet).

As per claim 27, Pearce et al. disclose a two-part device with a physical unit and a virtual unit comprising:

a physical unit having an ownership activation trigger for initiating, by a user, an activation signal from the physical unit to the virtual unit to activate an ownership procedure (see column 5, lines 33-41; see figure 2, items 32 and 100; the customer is prompted to enter a portion of the product ID of the software product to activate the software to combine that portion with another portion already included in the software program starting registration of the software product with a registration authority); and

the virtual unit, which communicates with the physical unit upon activation (see column 6, lines 23-26; figure 4, step 154; receiving the 15-bit product ID to concatenate with the 5-bit hardware ID);

in which the physical unit and the virtual unit employ a double safety mechanism to register ownership services (see column 6, lines 23-29; figure 4, step 154; a software product sending a 20-bit value over a network to a registration server to register itself with a registration authority; see column 5, lines 45-56; registering the software product for

installation and use on the computer) using a double knowledge check-proof of knowledge check mechanism (see column 6, lines 23-26; figure 4, step 154; where the 20-bit value is derived from the concatenation of a 15-bit product ID and a 5-bit hardware ID, each representative of distinct information and proof of knowledge of that information: see column 5, lines 46-46; figure 4, step 150; a first Knowledge Element of information that identifies the software product, place of manufacture, and serial number and a first Proof of Knowledge Check Element manifested by a product ID consisting of a 5-bit registered product code value, a 3-bit site value indicating the place of manufacture, and a 7-bit serialized number incremented with each product; see column 5, lines 57-67; column 6, lines 1-15; TABLE 1; figure 4, step 152; a second Knowledge Element of information that identifies a set of hardware components that make up the customer's computer and a second Proof of Knowledge Check Element represented by hardware ID (H/W ID) comprised of a bit sequence with the bit position indicative of the kind of component and a bit value indicative of an identifier of the component).

As per claim 28, Pearce et al. also describes:

that the virtual unit is a virtual device hosting entity that is one of: an Internet Data Center, and e-Services Host, a Control Console, and a Secure Data Storage Unit (see column 4, lines 13-25; the software enables the computer to function as handheld computer, a Web-enabled television, an automation system within the privacy of the home).

As per claim 29, Pearce et al. further points out:

that the Control Console is a web enabled browser (see column 4, lines 13-15; the software enables the computer to function as a Web-enabled television).

As per claim 30, Pearce et al. then elaborates:

that the Secure Data Storage Unit is a memory controllable by the user (see column 4, lines 27-38; figure 3, item 42; the customer computer contains system memory).

As per claim 31, Pearce et al. then elaborates:

that the Secure Data Storage Unit is a physical device under control by the user (see column 4, lines 27-38; figure 3, item 42; the customer computer contains system memory).

As per claim 32, Pearce et al. also suggests:

that the Secure Data Storage Unit is a virtual device under control by the user (see column 4, lines 49-53; nonvolatile storage of computer readable instructions, data structures, program modules and other data).

As per claims 33-36, Pearce et al. further point out:

that the virtual unit is activated and in the double safety mechanism, a first processor in the physical unit generates a first Knowledge Element and a first Proof of Knowledge Check Element (see column 5, lines 46-56; figure 4, step 150; performing on the customer's computer a first Knowledge Element of information that identifies the software product, place of manufacture, and serial number and a first Proof of Knowledge Check Element manifested by

a product ID consisting of a 5-bit registered product code value, a 3-bit site value indicating the place of manufacture, and a 7-bit serialized number incremented with each product), stores the first Knowledge Element in a Secure Storage Unit (see column 5, lines 52-56; storing the registered product code for the software product, the site value indicating the place of manufacture, and the serial number for the product in a secure memory in the computer) and sends the Proof of Knowledge Check Element to the virtual unit (see column 6, lines 23-26; figure 4, step 154; receiving the 15-bit product ID to concatenate with the 5-bit hardware ID), which authenticates (see column 6, lines 23-26; figure 4, step 154; concatenating the15-bit product ID with the 5-bit hardware ID where the 15-bit product ID must be in a proper format for authentication), and stores the Proof of Knowledge Check Element in an Ownership Proof of Knowledge Check Store (see column 6, lines 23-29; storing the 15-bit product ID in a memory for concatenation with the 5-bit hardware ID) and a second processor in the virtual unit generates a second Knowledge Element and a second Proof of Knowledge Check Element (see column 5, lines 57-67; column 6, lines 1-15; TABLE 1; figure 4, step 152; a second Knowledge Element of information that identifies a set of hardware components that make up the customer's computer and a second Proof of Knowledge Check Element represented by hardware ID (H/W ID) comprised of a bit sequence with the bit position indicative of the kind of component and a bit value indicative of an identifier of the component), in which

the second Proof of Knowledge Check Element is stored in an Ownership Knowledge Element Storage Unit (see column 6, lines 52-55; storing in system memory accessible by the software program); and the virtual unit sends the second Proof of Knowledge Check Element to the physical unit (see column 6, lines 48-50; figure 4, step 160; sending the hardware ID

processed into a registration ID to the customer computer), which authenticates and stores the second Proof of Knowledge Check Element in a second Proof of Knowledge Check Store unit (see column 6, lines 52-55; storing in system memory accessible by the software program).

As per claims 37 and 38, Pearce et al. then discusses:

utilizing an Internet address recorded in the physical unit to the activation signal (see column 6, lines 16-26; sending the product ID to a registration server over the Internet).

As per claim 39, Pearce et al. discloses a system for taking ownership of a part-physical, part-virtual device, comprising:

an activation trigger, located on a physical unit of the device, for initiating an activation signal (see column 5, lines 33-41; see figure 2, items 32 and 100; the customer is prompted to enter a portion of the product ID of the software product to activate the software to combine that portion with another portion already included in the software program starting registration of the software product with a registration authority);

the physical unit of the system, coupled to the activation trigger, for sending the activation signal to a virtual unit of the system (see column 5, lines 33-41; see figure 2, items 32 and 100; the customer is prompted to enter a portion of the product ID of the software product to activate the software to combine that portion with another portion already included in the software program starting registration of the software product with a registration authority); and

the virtual unit of the system, arranged to communicate with the physical unit of the

system, for registering ownership of the device using a double knowledge check-proof of knowledge mechanism (see column 6, lines 23-26; figure 4, step 154; receiving the 15-bit product ID to concatenate with the 5-bit hardware ID; see column 6, lines 23-29; figure 4, step 154; a software product sending a 20-bit value over a network to a registration server to register itself with a registration authority; see column 5, lines 45-56; registering the software product for installation and use on the computer) using a double knowledge check-proof of knowledge check mechanism (see column 6, lines 23-26; figure 4, step 154; where the 20-bit value is derived from the concatenation of a 15-bit product ID and a 5-bit hardware ID, each representative of distinct information and proof of knowledge of that information: see column 5, lines 46-56; figure 4, step 150; a first Knowledge Element of information that identifies the software product, place of manufacture, and serial number and; see column 6, lines 39-41; figure 4, step 156; a first Proof of Knowledge Check Element as a registration ID computed from the product ID and hardware ID; see column 5, lines 57-67; column 6, lines 1-15; TABLE 1; figure 4, step 152; a second Knowledge Element of information that identifies a set of hardware components that make up the customer's computer and a second Proof of Knowledge Check Element represented by hardware ID (H/W ID) comprised of a bit sequence with the bit position indicative of the kind of component and a bit value indicative of an identifier of the component).

As per claim 40, Pearce et al. also describes:

that the virtual unit is a virtual device hosting entity that is one of: an Internet Data Center, and e-Services Host, a Control Console, and a Secure Data Storage Unit (see column 4,

lines 13-25; the software enables the computer to function as handheld computer, a Web-enabled television, an automation system within the privacy of the home).

As per claim 41, Pearce et al. further points out:

that the Control Console is a web enabled browser (see column 4, lines 13-15; the software enables the computer to function as a Web-enabled television).

As per claim 42, Pearce et al. then elaborates:

that the Secure Data Storage Unit is a memory controllable by the user (see column 4, lines 27-38; figure 3, item 42; the customer computer contains system memory).

As per claim 43, Pearce et al. then elaborates:

that the Secure Data Storage Unit is a physical device under control by the user (see column 4, lines 27-38; figure 3, item 42; the customer computer contains system memory).

As per claim 44, Pearce et al. also suggests:

that the Secure Data Storage Unit is a virtual device under control by the user (see column 4, lines 49-53; nonvolatile storage of computer readable instructions, data structures, program modules and other data).

As per claim 45, Pearce et al. further point out:

that the virtual unit is activated and in the double safety mechanism, a first processor in

the physical unit generates a first Knowledge Element and a first Proof of Knowledge Check Element (see column 5, lines 46-56; figure 4, step 150; performing on the customer's computer a first Knowledge Element of information that identifies the software product, place of manufacture, and serial number and a first Proof of Knowledge Check Element manifested by a product ID consisting of a 5-bit registered product code value, a 3-bit site value indicating the place of manufacture, and a 7-bit serialized number incremented with each product), stores the first Knowledge Element in a Secure Storage Unit (see column 5, lines 52-56; storing the registered product code for the software product, the site value indicating the place of manufacture, and the serial number for the product in a secure memory in the computer) and sends the Proof of Knowledge Check Element to the virtual unit (see column 6, lines 23-26; figure 4, step 154; receiving the 15-bit product ID to concatenate with the 5-bit hardware ID), where the virtual unit validates the identity of the physical unit using a proof of knowledge check that corresponds to a knowledge element of the physical unit (see column 6, lines 23-26; figure 4, step 154; concatenating the15-bit product ID with the 5-bit hardware ID where the 15-bit product ID must be in a proper format for authentication), and stores the Proof of Knowledge Check Element in an Ownership Proof of Knowledge Check Store (see column 6, lines 23-29; storing the 15-bit product ID in a memory for concatenation with the 5-bit hardware ID) and a second processor in the virtual unit generates a second Knowledge Element and a second Proof of Knowledge Check Element (see column 5, lines 57-67; column 6, lines 1-15; TABLE 1; figure 4, step 152; a second Knowledge Element of information that identifies a set of hardware components that make up the customer's computer and a second Proof of Knowledge Check Element represented by hardware ID (H/W ID) comprised of a bit sequence

with the bit position indicative of the kind of component and a bit value indicative of an identifier of the component), in which

the second Proof of Knowledge Check Element is stored in an Ownership Knowledge Element Storage Unit (see column 6, lines 52-55; storing in system memory accessible by the software program); and the virtual unit sends the second Proof of Knowledge Check Element to the physical unit (see column 6, lines 48-50; figure 4, step 160; sending the hardware ID processed into a registration ID to the customer computer), where the physical unit validates the identity of the virtual unit using a proof of knowledge check that corresponds to a knowledge element of the virtual unit (see column 6, lines 52-55; storing in system memory accessible by the software program).

As per claim 46, Pearce et al. further points out:

that ownership is registered when the physical unit communicates with the virtual unit via an Internet address associated with the virtual unit (see column 6, lines 48-55; figure 4, steps 160 and 162; the registration server returns the registration ID over the network accessible by the software program; see column 4, lines 21-23; figure 2, item 36; where the network is the Internet requiring the software program as an addressee to have an Internet address).

As per claim 47, Pearce et al. further point out:

that the virtual unit is activated and in the double safety mechanism, a first processor in the physical unit generates a first Knowledge Element and a first Proof of Knowledge Check Element (see column 5, lines 46-56; figure 4, step 150; performing on the customer's computer

a first Knowledge Element of information that identifies the software product, place of manufacture, and serial number and a first Proof of Knowledge Check Element manifested by a product ID consisting of a 5-bit registered product code value, a 3-bit site value indicating the place of manufacture, and a 7-bit serialized number incremented with each product), stores the first Knowledge Element in a Secure Storage Unit (see column 5, lines 52-56; storing the registered product code for the software product, the site value indicating the place of manufacture, and the serial number for the product in a secure memory in the computer) and sends the Proof of Knowledge Check Element to the virtual unit (see column 6, lines 23-26; figure 4, step 154; receiving the 15-bit product ID to concatenate with the 5-bit hardware ID), which authenticates (see column 6, lines 23-26; figure 4, step 154; concatenating the15-bit product ID with the 5-bit hardware ID where the 15-bit product ID must be in a proper format for authentication), and stores the Proof of Knowledge Check Element in an Ownership Proof of Knowledge Check Store (see column 6, lines 23-29; storing the 15-bit product ID in a memory for concatenation with the 5-bit hardware ID) and a second processor in the virtual unit generates a second Knowledge Element and a second Proof of Knowledge Check Element (see column 5, lines 57-67; column 6, lines 1-15; TABLE 1; figure 4, step 152; a second Knowledge Element of information that identifies a set of hardware components that make up the customer's computer and a second Proof of Knowledge Check Element represented by hardware ID (H/W ID) comprised of a bit sequence with the bit position indicative of the kind of component and a bit value indicative of an identifier of the component), in which

the second Proof of Knowledge Check Element is stored in an Ownership Knowledge Element Storage Unit (see column 6, lines 52-55; storing in system memory accessible by the

software program); and the virtual unit sends the second Proof of Knowledge Check Element to the physical unit (see column 6, lines 48-50; figure 4, step 160; sending the hardware ID processed into a registration ID to the customer computer), which authenticates and stores the second Proof of Knowledge Check Element in a second Proof of Knowledge Check Store unit (see column 6, lines 52-55; storing in system memory accessible by the software program).

As per claims 48-51, Pearce et al. then elaborates:

that a console is coupled to the virtual unit via a network connection and to a Secure Storage Unit (see column 4, lines 4-21; figure 2, items 34 and 36; the registration server interconnected by a network to a customer computer running the software product; see column 6, lines 44-46; figure 2, items 34 and 114; figure 4, step 158; wher the registration server maintains a database to store the product ID, hardware ID, and registration ID),

for maintaining a Knowledge Element Store and a Proof of Knowledge Check Store in the Secure Storage Unit (see column 6, lines 44-47; figure 2, items 34, 114, and 116; figure 4, step 158; where the registration server maintains a database with a portion for the product ID and hardware ID as a Knowledge Element Store and another portion for the registration ID as a Proof of Knowledge Store correlated with the product ID and hardware ID), and

upon user selection (see column 5, lines 39-40; the customer registers the software product with the registration authority), generating a first Knowledge Element (see column 5, lines 46-56; figure 4, step 150; generating a first Knowledge Element of information that identifies the software product, place of manufacture, and serial number) and a corresponding first Proof of Knowledge Check for the part-physical, part-virtual device (see column 6, lines

39-41; figure 4, step 156; computing the registration ID from the product ID and the hardware ID), storing the first Knowledge Element in the Secure Storage Unit (see column 6, lines 44-47; figure 2, items 34, 114, and 116; figure 4, step 158; where the registration server maintains a database with a portion for the product ID and hardware ID) and sending the first Proof of Knowledge Check to the virtual unit (see column 6, lines 48-55; figure 4, steps 160 and 162; the registration server returns the registration ID accessible by the software program).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Justin T. Darrow whose telephone number is (571) 272-3801, and whose electronic mail address is justin.darrow@uspto.gov. The examiner can normally be reached Monday-Friday from 8:30 AM to 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barrón, Jr., can be reached at (571) 272-3799.

The fax number for Formal or Official faxes to Technology Center 2100 is 571-273-8300. In order for a formal paper transmitted by fax to be entered into the application file, the paper and/or fax cover sheet must be signed by a representative for the applicant. Faxed formal papers for application file entry, such as amendments adding claims, extensions of time, and statutory disclaimers for which fees must be charged before entry, must be transmitted with an authorization to charge a deposit account to cover such fees. It is also recommended that the cover sheet for the fax of a formal paper have printed "**OFFICIAL FAX**". Formal papers

transmitted by fax usually require three business days for entry into the application file and consideration by the examiner. Formal or Official faxes including amendments after final rejection (37 CFR 1.116) should be submitted to 571-273-8300 for expedited entry into the application file. It is further recommended that the cover sheet for the fax containing an amendment after final rejection have printed not only "**OFFICIAL FAX**" but also "**AMENDMENT AFTER FINAL**".

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Any inquiry of a general nature or relating to the status of this application should be directed to the Group receptionist whose telephone number is (571) 272-2100.

December 12, 2005

Justin Darrow

JUSTIN T. DARROW
PRIMARY EXAMINER
TECHNOLOGY CENTER 2100